

SEALED

7:21mj163

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kathryn Weber, am a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent with the FBI since 2012. I am currently assigned to the Richmond Field Office investigating crimes against children. While employed by the FBI, I have investigated federal criminal violations related to child exploitation, child pornography, civil rights, white collar crimes, and others. I have gained experience through training provided by the FBI and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252 and 2252A, and I am authorized by law to request a search warrant.

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in Attachment A of this Affidavit, including the entire property located at 610 E CEDAR STREET, COVINGTON, VIRGINIA 24426 (the “SUBJECT PREMISES”) and the content of Computers, Computer hardware and electronic storage media located therein (including Computers, Computer hardware or electronic storage media located on the persons of anyone within the SUBJECT PREMISES at the time of the warrant’s execution), for contraband and

evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A, which items are more specifically described in Attachment B of this Affidavit.

3. The statements in this Affidavit are based in part on information provided by other sworn law enforcement officers participating in this investigation and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1) and (b)(1) (transportation of child pornography); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (distribution and/or receipt of child pornography) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:
 - a. 18 U.S.C. §§ 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.
 - b. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in

18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

- c. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the

visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP

addresses can be “dynamic,” meaning that the internet service provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

g. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

h. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

i. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

j. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

k. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of

conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. The instant investigation involves a user of “Freenet” — which is an Internet-based, peer-to-peer (P2P) network that allows users to anonymously share files, chat on message boards, and access websites within the network. Law enforcement agents have been investigating child pornography trafficking by Freenet users since at least 2011.

Background Regarding Freenet

7. In order to access Freenet, a user must first download the Freenet software, which is free and publicly available. The Freenet “source code” — i.e., the computer programming code that enables Freenet’s operation — is also publicly available. In other words, Freenet is “open source” software that may be examined and analyzed by anyone with the pertinent expertise or knowledge. There is also Freenet Mobile application that may be installed on Android mobile phone devices.

8. Anyone running the Freenet software may join and access the Freenet network. Each computer running Freenet connects directly to other computers running Freenet, which are called its “peers.”¹ When installing Freenet, each user agrees to provide to the network a portion of the storage space on the user’s computer hard drive, so that files uploaded by Freenet users can be distributed and stored across the network. Freenet users can upload files into the Freenet network and download files from the Freenet network. After a user installs Freenet on their

¹ The number of peers is determined by the user’s settings and is based on the quality and speed of the user’s Internet connection.

computer, the software creates a default “download” folder. If a user successfully downloads a particular file from Freenet, Freenet may save the content of that file to the “download” folder. A user may change this default setting and direct the content to be downloaded elsewhere.

9. When a user uploads a file into Freenet, the software breaks the file into pieces, called “blocks,” and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored throughout the Freenet network of peers.² The software also creates an index piece that contains a list of all the pieces of the file and a unique key – a series of letters, numbers and special characters – that is used to download the file.³

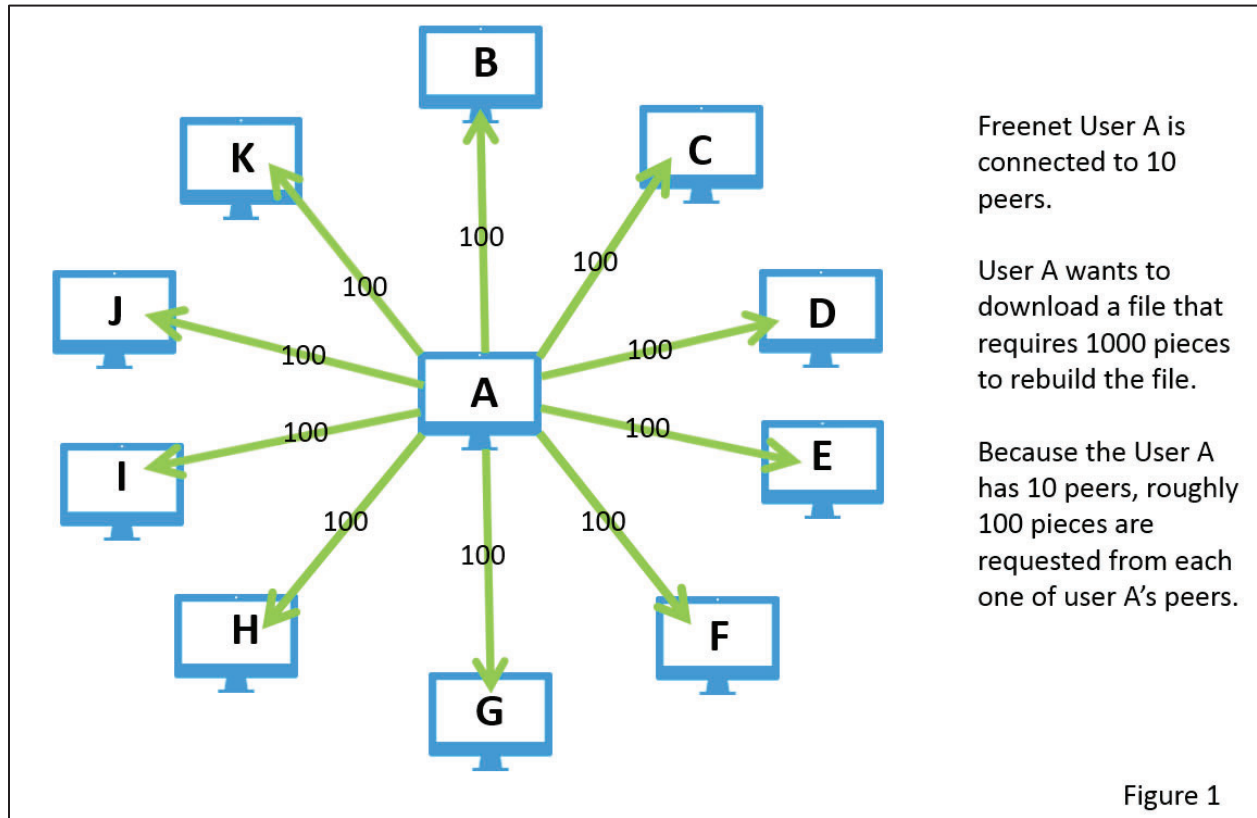
10. In order to download a file on Freenet, a user must have the key for that file. There are a number of ways that a Freenet user can download a file using a key. Some examples include: (1) the “download” box on Freenet’s “file sharing” page; (2) the “download” box on the message board associated with Freenet or other Freenet add-on programs; and (3) directly through the user’s web browser while the user is connected to the Freenet network.

11. When a user attempts to download a file via Freenet, Freenet downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file. The Freenet software then requests all of the pieces of the file from the user’s peers. Rather than request all of the file pieces from a single peer, requests for file pieces are divided up in roughly equal amounts among the user’s peers. If a user’s peer does not

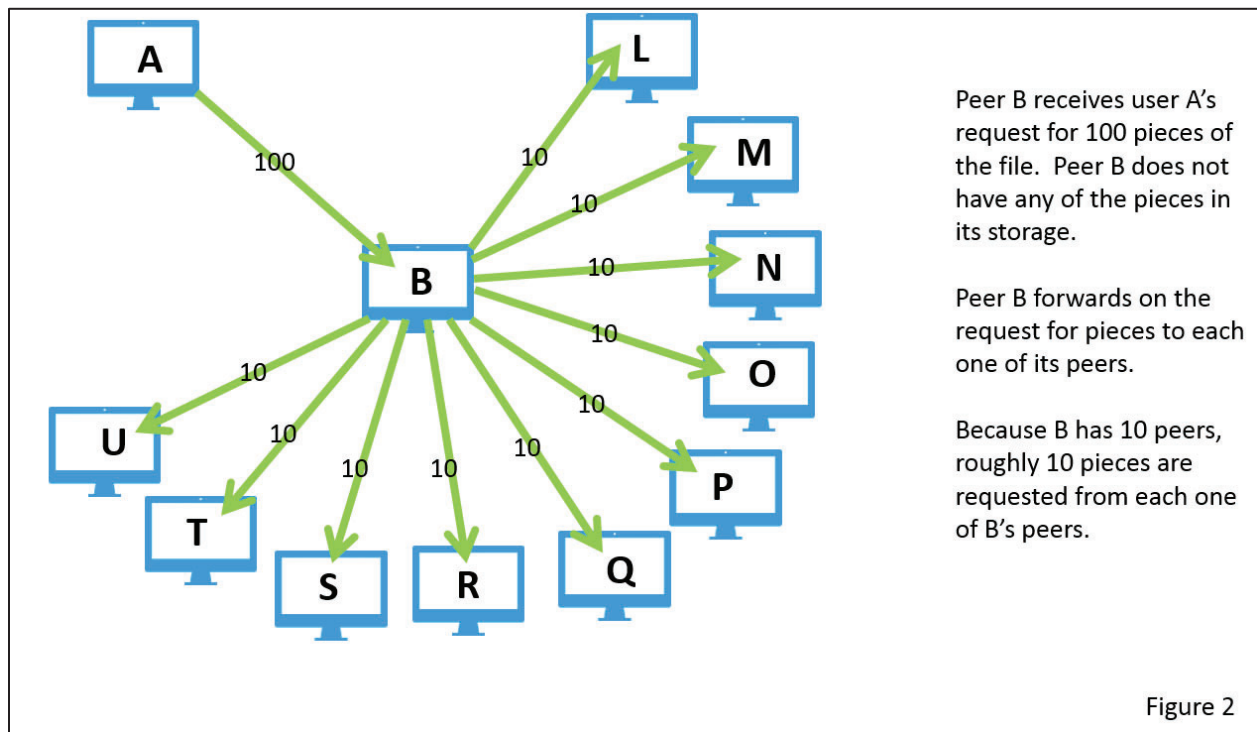
² Because the pieces of files are encrypted, a Freenet user is unable to access the content of pieces that are stored on the user’s own computer hard drive because they are not in a readable format.

³ An example key is: CHK@0R6h6o8a~JbOGg8GmxGauRyqJPSwcHGmxGauLznw8FeyB0go,08agxRpNx~wc~rmZRfWQaSed3HTeKKkXAwvDRF2LUaU,AAMC--8/lolitaz49.avi.

have the particular requested pieces in its storage, that peer will then divide up and ask its peers for the pieces, and so on. For example, if User “A” has 10 peers and requests 1000 pieces of a file, roughly 100 pieces are requested from each one of User A’s peers. See Figure 1.



If Peer “B” receives User A’s request for 100 pieces of the file, but does not have any of those pieces in its storage, Peer B forwards on the request for those pieces to Peer B’s peers. If Peer B has 10 peers of its own, roughly 10 pieces are requested from each one of Peer B’s peers. See Figure 2.



As noted below, this design can help law enforcement distinguish between a Freenet user that is the original requestor of a file, and one that is merely forwarding the request of another user.

12. To prevent requests for pieces from going on indefinitely, Freenet is configured to only allow a request for a piece of a file to be forwarded to another peer a limited number of times (the default maximum is 18). If a request reaches that limit without finding the requested piece, a signal is returned to the user's computer and the request is sent to another of the user's peers. The remaining number of times a request for a piece may be forwarded is included within the request for that piece.

13. Freenet attempts to hide which computer uploaded a file into or downloaded a file from the network by making it difficult to differentiate whether a request for a piece that comes in from a peer originated with that peer (i.e., the peer was the "original requestor" of the file), or whether that peer was simply forwarding a different peer's request. Freenet attempts to hide the

identity of the original requestor by randomizing the initial number of times a request can be forwarded from one peer to another to be either 17 or 18. Without this randomization, any time a user received a request for a piece of a file that could be forwarded 18 times, the user would know that its peer was the original requestor of the file. This design allows investigators using Freenet to focus investigative efforts on peer computers that request pieces of files of interest that may be forwarded 17 or 18 times, in order to determine whether the peer was the original requestor of the file.

14. Freenet has two operational modes, “Darknet” and “Opennet.” On the Darknet mode, a computer connects only to peers whom the user has specifically selected. On the Opennet mode, a computer may connect to peers unknown to the user. A Freenet user may choose which mode to use. The mode relevant to this investigation involves a user who chose to use the Opennet operational mode.

15. Freenet warns its users in multiple ways that it does not guarantee anonymity: when Freenet software is initially installed; within the log file each time Freenet is started; and via Freenet’s publicly accessible website. Freenet software also does not mask a computer’s IP address — the IP addresses of each Freenet user’s peers are observable to the user. For example, if a user is connected to 10 peers on Freenet, all 10 of those peers’ IP addresses will be observable to the user. The fact that Freenet does not mask IP addresses is explained on its publicly accessible website. Freenet also acknowledges on its publicly accessible website that, for users who use the Opennet mode, it can be statistically shown that a particular user more likely than not requested a file (as opposed to having merely forwarded the request of another

peer) based on factors including the proportion of the pieces of a file requested by a user and the number of nearby peers.

16. There is also a Freenet Mobile application available to the users of Android mobile devices.

Child Pornography Images/Videos on “Freenet”

17. Freenet can be used to advertise and distribute images and videos of child pornography. Unlike other file sharing systems, Freenet does not provide a search function for its users whereby users would insert search terms to locate files. A user who wishes to locate and download child pornography from Freenet must identify the key associated with a particular child pornography file and then use that key to download the file.

18. Freenet users can identify those keys in a number of ways. For example, “message boards” exist on Freenet that allow users to post textual messages and engage in online discussions involving the sexual exploitation of minors. Law enforcement agents have observed message boards labeled with terms known to be associated with child pornography, including: “pthc” (an acronym for “pre-teen hard core”), “boy porn,” “hussy,” “pedomom,” “kidfetish,” “toddler_cp,” “hurtcore,” and “tor-childporn.” Typical posts to those message boards contain text, keys of child pornography files that can be downloaded through Freenet, and in some cases descriptions of the image or video file associated with those keys.

19. Freenet users can also obtain keys of child pornography images or videos from websites that operate within Freenet called “Freesites.” Freesites can only be accessed through Freenet. Some of those sites contain images of child pornography the user can view along with

keys of child pornography files. It is also possible that Freenet users may obtain keys related to child pornography images or videos directly from other Freenet users.

Investigation into the Trafficking of Child Pornography on Freenet

20. Since approximately 2011, law enforcement has been investigating the trafficking of child pornography on Freenet. A modified version of the Freenet software is available to sworn law enforcement officers to assist in conducting Freenet investigations. I have been trained on the operation of the modified law enforcement version of Freenet. This law enforcement version is nearly identical to Freenet, except that it allows a computer operated by a law enforcement officer to automatically log information about requests for pieces of files received directly from its peers. The types of information logged by a law enforcement computer are available to all standard Freenet users as part of Freenet's normal operation. This information includes but is not limited to: the IP addresses of the user's peers; the number of peers those peers report to have; a unique identifier assigned by the software (referred to as the computer's Freenet "location"); the remaining number of times a request for a piece of a file may be forwarded; the date/time of requests received from a peer; and the digital hash value of a requested piece.

21. Law enforcement computers do not target specific peers on Freenet nor do law enforcement computers solicit requests from any peers. The Freenet information collected by law enforcement computers is logged and provided to other Freenet-trained law enforcement personnel to further investigations into Freenet users believed to be downloading child pornography files through Freenet.

22. Law enforcement officers collect keys associated with suspected child pornography files that are being publicly shared and advertised on Freenet. Law enforcement only investigates Freenet users who request pieces of files associated with such keys collected by law enforcement. The keys collected by law enforcement have been obtained via publicly accessible sites, such as Freenet message boards and Freesites, as well as during prior investigations into child pornography trafficking on Freenet. This investigation pertains to child pornography files with known keys, the content of which are further described below. Those files are referenced as “files of interest.”

23. By viewing the documented activity of a peer that sends a request to a law enforcement computer, it is possible to determine whether it is significantly more probable than not that the peer is the original requestor of a file of interest. Only those requests that were intended for law enforcement computers as recipients, that may be forwarded 17 or 18 times, and are associated with a file of interest are analyzed. A mathematical formula is then applied to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request of another computer.

24. Your affiant has reviewed a peer-reviewed, publicly available academic paper describing the methodology of that mathematical formula. In basic terms, the methodology relies on two primary facts about the Freenet software. First, the original requestor divides up its requests for pieces of a file among its peers, sending a roughly equal fraction of the requests to each peer. Second, if a peer does not have the requested pieces, the peer takes the fraction of requests for pieces of a particular file and divides them up again among its own peers. See

Figures 1 and 2. Because a peer that is merely routing another peer's request would ask its peers for a significantly smaller portion of the pieces of a file than an original requester, it is possible for the recipient of requests to determine whether a request is significantly more likely than not from an original requestor. The academic paper's detailed evaluation finds that a formal mathematical formula based on this reasoning is highly accurate (specifically, it has a high true positive rate and a low false positive rate).⁴ Based upon my training and experience, I believe this to be a reliable method to determine whether it is significantly more probable than not that a given Freenet computer is the original requestor of a file of interest.

25. I am also aware through my training and experience that dozens of searches of digital devices have been conducted by law enforcement officers (either through court-authorization or consent) related to targets whose IP addresses were identified based upon analysis of information from Freenet law enforcement computers. The vast majority of those searches yielded evidence of child pornography possession and/or trafficking in child pornography.

Requests Targeted in the Instant Investigation

26. I have reviewed information obtained and logged by law enforcement computers running the Freenet software related to IP address 216.98.95.172. Such information shows that a Freenet user with IP address 216.98.95.172 requested pieces of the child pornography files described below from a law enforcement Freenet computer. With respect to each file – considering the number of requested file pieces, the total number of file pieces required to

⁴ Your affiant can make that academic paper available to the court upon request.

assemble the file, and the number of peers the user had – the number of requests for file pieces is significantly more than one would expect to see if the user of IP address 216.98.95.172 were merely routing the request of another user. Accordingly – based on my review of those records, the application of the methodology described above, my understanding of Freenet, my training and experience, and the fact that the same user requested pieces of multiple child pornography files – I believe that the user of IP address 216.98.95.172 was the original requestor of each of the described files.

27. On July 3, 2021, between 6:19 PM UTC⁵ and 10:58 PM UTC, a computer running Freenet software, with an IP address of 216.98.95.172, with an average of 23.7 peers, requested from a law enforcement computer 111 pieces out of 3,538 total pieces needed to assemble a file with a SHA1 digital hash value of

X3CDZ6VITZOQ3YN22AIR5F4RGFJYDDNE.⁶ I have downloaded the exact same file with

⁵ Coordinated Universal Time or UTC is the primary time standard by which the world regulates clocks and time. It is within about 1 second of mean solar time at 0° longitude and is not adjusted for daylight saving time. It is effectively a successor to Greenwich Mean Time (GMT), which is a time zone used by a few countries in Africa and Western Europe, including the UK during winter.

⁶ “SHA1” stands for “secure hash algorithm – 1” and refers to a particular type of cryptographic hash value. Hash values can be thought of as fingerprints for files. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value – the hash value - is produced that identifies the contents of the file. Hash values are widely used in computer programs and digital technologies to verify data file identity and integrity. Hash values are unique, and the possibility of two different files have the same hash value, something called a “hash collision,” is staggeringly small. Hash files are also reproducible, i.e., the same file, if unaltered, will always generate the same hash value when the same hash algorithm is used. But if the contents are modified in any way, the value of the hash will also change significantly. There are several types of hash algorithms, including MD-5, SHA-1, and SHA-256, to name a few.

the above referenced SHA1 hash value from Freenet. It is a video approximately 9 minutes and 3 seconds in duration titled “Linda Full.mpg.” The video initially depicts a naked female minor and the naked lower half of a male body, including male genitals. Based on my training and experience, the child is prepubescent and appears to be 8 to 10 years old. Throughout the video, the female minor licks and sucks on the male penis from different angles. Ultimately, the male ejaculates in the female minor’s mouth and the female minor swallows the ejaculate.

28. On August 7, 2021, from 1:54 PM UTC through 4:06 PM UTC, a computer running Freenet software, with the same IP address of 216.98.95.172, having an average of 41.0 peers, requested from a law enforcement computer 98 pieces out of 3,692 total pieces needed to assemble a file with a SHA1 digital hash value of RZI7XU5DWUR2OOVHH5LC4NXAUUHREW2V. I have downloaded the exact same file with the above referenced SHA1 hash value from Freenet. It is a video approximately 9 minutes and 48 seconds in duration titled “(pthc) NEW 2016 Pedo Childlover 8yo Daddy%27s Little Girl JM 06.mp4.” The video depicts a clothed, female minor on her stomach between the legs of an adult male. The female minor is facing the camera and the adult male’s penis can be seen in the foreground of the video. Based on my training and experience, the child is prepubescent and appears to be 7 to 9 years old. Throughout the video, the female minor holds and sucks on the male penis. At one point in the video, while the male masturbates, the female minor appears to suck on the male’s scrotum. Towards the end of the video, the male appears to ejaculate into the female minor’s mouth.

29. On August 7, 2021, between 1:59 PM UTC and 4:47 PM UTC, a computer running Freenet software, again with an IP address of 216.98.95.172, with an average of 40.9

peers, requested from a law enforcement computer 154 pieces out of 5,561 total pieces needed to assemble a file with a SHA1 digital hash value of 4BVM5FJX4UM64I2NJ2UJF7XUJSARN7B4. I have downloaded the exact same file with the above referenced SHA1 hash value from Freenet. It is a video approximately 10 minutes and 43 seconds in duration titled “(pthc) NEW 2016 Pedo Childlover 8yo Daddy%27s Little Girl JM 10.mp4.” The video initially depicts a naked female minor and an adult male. Based on my training and experience, the child is prepubescent and appears to be 7 to 9 years old. Throughout the video, the adult male licks the female minor’s genitals, the female minor sucks the adult male’s penis, the adult male touches his penis to the female minor’s genitals, and ultimately ejaculates on the female minor’s face.

30. The fact that a Freenet user requested pieces associated with a particular file on Freenet indicates that the user attempted to download the file’s contents from Freenet. It does not indicate whether or not the user successfully retrieved all of the necessary pieces to successfully download the file.

31. Based on my training and experience, I am aware that downloaders and consumers of child pornography retain these images and often form large collections. Therefore, based on this knowledge I believe there is probable cause that the images downloaded in July 2021 and August 2021, along with other images of child pornography, will still be present in the SUBJECT PREMISES.

32. The keys for each of these files were obtained by law enforcement agents at some point between 2011 and the present date. The source for these file keys was either from a Freenet message board or Freesite that contained information related to the sexual exploitation of

children, or from a previous investigation. I am not aware of how, or from where, this particular Freenet user obtained the keys used to attempt to retrieve the files of interest described.

Identification of the SUBJECT PREMISES

29. Using publicly available search tools, law enforcement determined that IP address 216.98.95.172 was controlled by Internet Service Provider (“ISP”) Lumos Networks.

30. On or about August 20, 2021, an FBI administrative subpoena was served on Lumos Networks for subscriber information relating to the use of IP address 216.98.95.172 on July 3, 2021, at 18:19:09 UTC and 22:58:13 UTC, and on August 7, 2021, at 13:55:09 UTC, 15:19:37 UTC, 13:59:50 UTC, and 16:47:23 UTC. A review of the results obtained on or about September 16, 2021, revealed the following account holder, Jerald Gray, and address, which is the address of the SUBJECT PREMISES: 610 E CEDAR STREET, COVINGTON, VIRGINIA 24426.

31. A review of Covington, Virginia, GIS records identified Jerald Gray as the owner of the SUBJECT PREMISES.

32. A check with the Department of Motor Vehicles on or about November 9, 2021, revealed that an individual named Jerald Francis Gray with a date of birth of April 6, 1972 resides at the SUBJECT PREMISES.

33. Surveillance of the SUBJECT PREMISES on or about November 5, 2021, identified a Honda Civic with Virginia license plate UCH-6544 parked near the front of the SUBJECT PREMISES. According to the Department of Motor Vehicles, this vehicle is registered to Jerald Francis Gray at the SUBJECT PREMISES. On the same date, a female was observed driving the aforementioned vehicle. The back side of an adult male was observed

entering the front door of the SUBJECT PREMISES. The appearance of the adult male's size was consistent with the DMV information and photograph for Jerald Francis Gray.

34. A review of a Covington Police Department Report from on or about September 20, 2021, revealed the aforementioned Honda Civic with Virginia license plate UCH-6544 registered to Jerald Francis Gray was involved in a traffic stop. The driver of the vehicle at the time of the traffic stop was identified as Stephanie Dawn Gray. The police report lists Stephanie Dawn Gray's address as the SUBJECT PREMISES. Additionally, a check with the Department of Motor Vehicles on or about November 17, 2021, revealed that an individual named Stephanie Dawn Gray with a date of birth of February 18, 1993 resides at the SUBJECT PREMISES.

35. In June 2005, a minor victim reported to Covington Police Department (Virginia) that she was fondled by Jerald Gray. The victim was awakened two times by Gray. In the first incident Gray was kissing on her breasts. In the second incident Gray grabbed the victim's buttocks. The victim and the friend she was visiting then stayed up the rest of the night. In November 2005 Covington Police Department put the case into inactive status because they could not locate Gray.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS,
AND THE INTERNET

36. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically

serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it

(or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or

“footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

37. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a Computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of Computers, Computer hardware and electronic storage media, a search of the data on such devices or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B). A common place that Computers such as mobile phones can be found is on a person (such as in a person’s pocket). Thus, the warrant applied for would authorize the seizure, search and copying of Computers, Computer hardware and electronic storage media found on a person located within the SUBJECT PREMISES at the time of the warrant’s execution in the same manner as devices found elsewhere within the SUBJECT PREMISES.

38. I submit that if a Computer, Computer hardware or electronic storage medium is found on the SUBJECT PREMISES, there is probable cause to believe the records stored on that device will include evidence, fruits and instrumentalities of the crimes listed above for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when

files have been deleted, they can be recovered months or years later using forensic tools.

This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

39. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how Computers were used, the

purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any Computer. Computer hardware or electronic storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or

controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates

to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, pieces, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

40. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of

the technical manuals and specialized equipment necessary to conduct a thorough search.

In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a

“dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

41. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called “wireless routers,” which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be “secured” (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or “unsecured” (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

42. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, searching, imaging, or otherwise copying Computers, Computer hardware and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

43. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

44. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

/s/ Kathryn Weber
Kathryn Weber
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me, by telephone, this 3rd day of December, 2021.

Robert S. Ballou

ROBERT S. BALLOU
UNITED STATES MAGISTRATE JUDGE

7:21mj163

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at 610 E CEDAR STREET, COVINGTON, VIRGINIA 24426, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). The house number of 610 is visible on the far right post of the porch when looking at the SUBJECT PREMISES from the street. The following are images of the SUBJECT PREMISES:



7:21mj163

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C.

§§ 2252 and 2252A:

1. Computers, Computer hardware or electronic storage media used as a means to commit the violations described above, including such devices found on persons within the SUBJECT PREMISES during the execution of the search warrant, or found anywhere else in the SUBJECT PREMISES.
2. For any Computer, Computer hardware or electronic storage medium whose seizure is otherwise authorized by this warrant, and any Computer. Computer hardware or electronic storage medium, including mobile phones that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):
 - a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence

of the presence or absence of security software designed to detect malicious software;

- c. Evidence of the lack of such malicious software;
- d. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. Evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
- f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. Evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. Evidence of the times the COMPUTER was used;
- i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. Records of or information about Internet Protocol addresses used by the COMPUTER;
- l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

- m. Contextual information necessary to understand the evidence described in this attachment.
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
- 4. Child pornography and child erotica.
- 5. Records, information, and items relating to violations of the statutes described above including:
 - a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 610 E CEDAR STREET, COVINGTON, VIRGINIA 24426, including utility and telephone bills, mail envelopes, or addressed correspondence;
 - b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
 - c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
 - d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of Internet-based websites, message boards, databases and discussion forums related to child exploitation; and

- e. Records and information showing access to and/or use of Internet-based websites, message boards, databases and discussion forums related to child exploitation.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.